



# **ETA and Trustwave Present:**

## **PCI DSS Compliance and the Level 4 Merchant Population: Supporting Small Merchants**

**June 26, 2008**

Presented by:

Jami Taylor, VP-Alliance and Channel Partners, Trustwave  
Don Roeber, Merchant Compliance Manager, Vice President, Fifth Third  
Processing Solutions





## Before We Get Started...

- **Please remember to call-in to the audio portion of the presentation.  
(VoIP functionality is not available for this webinar.)  
Call: 650-429-3300 or 866-469-3239  
Enter meeting number: 352 838 647**
- **If you have questions for the presenter, please submit them to the host using the chat box in the lower right corner of your screen. Questions will be answered during a Q&A session following the presentation.**



# The Need



# What is a Credit Card Compromise?

**An unauthorized individual taking advantage of a flaw in a system that:**

Processes, transmits or stores  
cardholder data



**To gain access to:**

- Card Numbers
- Expiration Dates
- CVV2/CVC2/CID
- Track Data





# Non-Compliance: Risks, Fines, Fees, Costs, Loss

## **A compromised organization that is found to be non-compliant could expect the following:**

- Damage to their brand/reputation
- Costs
  - Investigation
  - Remediation
- Non-Compliance fines
- Re-Issuance fees
- Fraud loss
- Ongoing compliance audits
- Victim notification costs

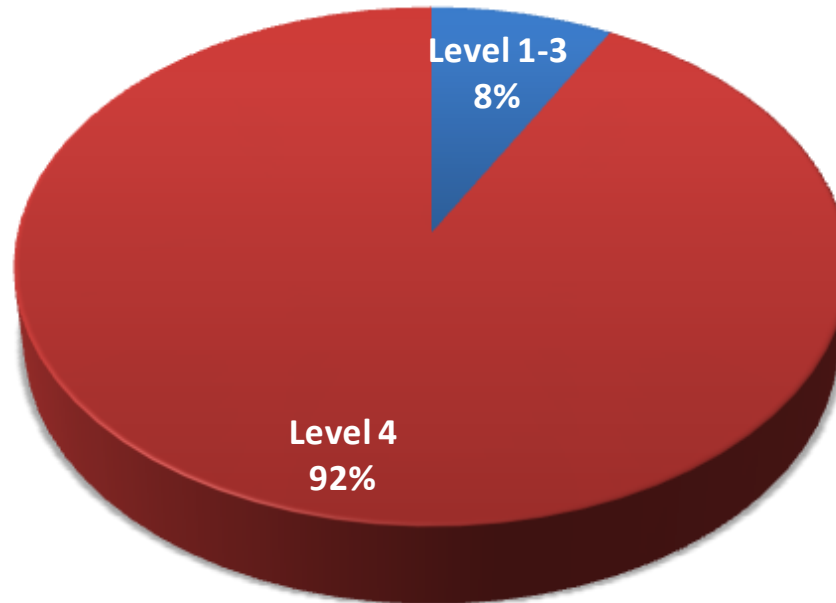


# Compromise Statistics



# Case Analysis: Merchant Level

**While larger merchants represent greater transaction volume, smaller merchants have greater risk due to many factors discussed in this presentation.**

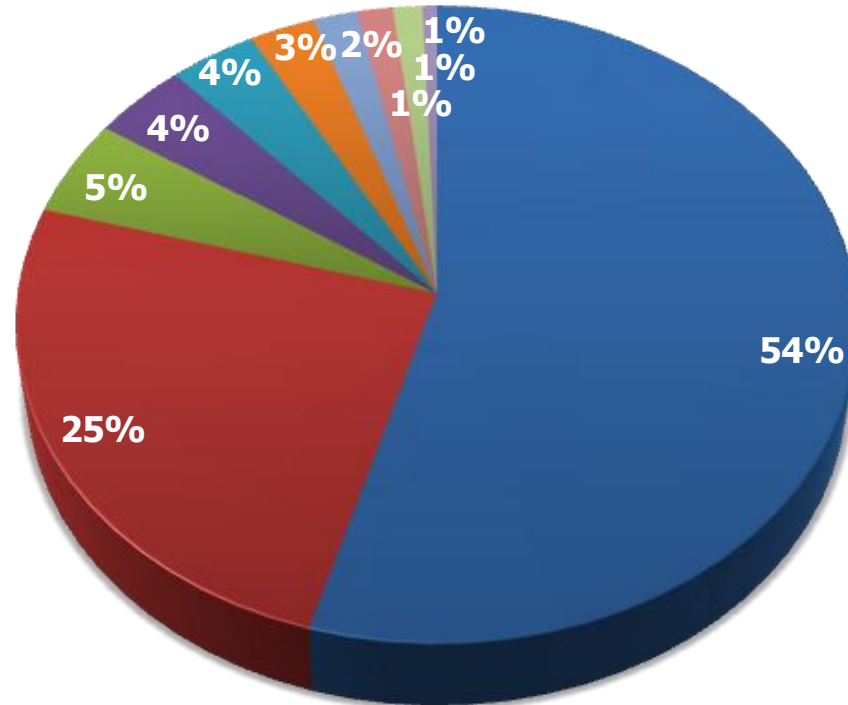


**Trustwave's analysis is derived from more than 350 cardholder data compromise investigations performed in over 14 different countries.**



# Case Analysis: Industry

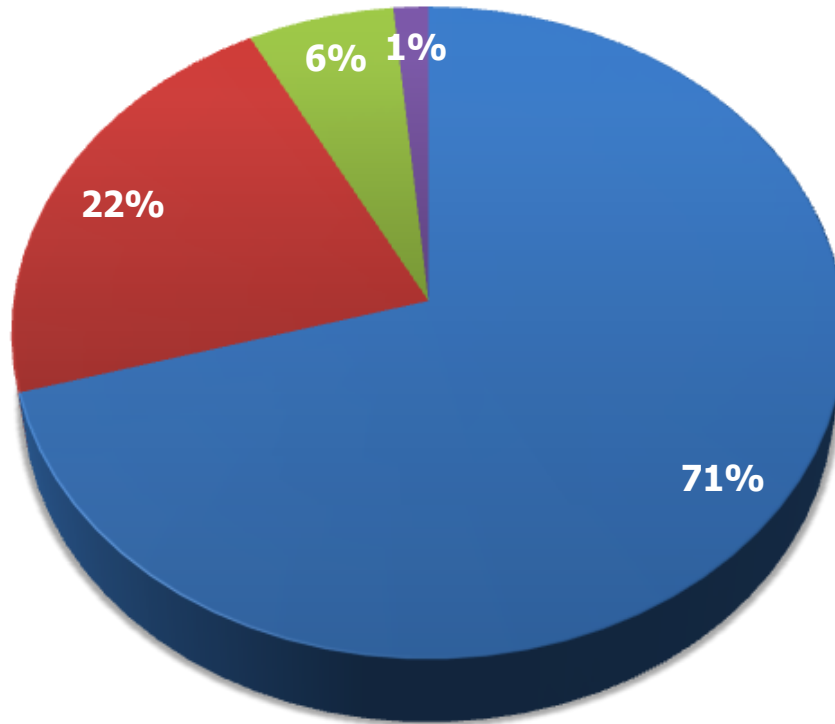
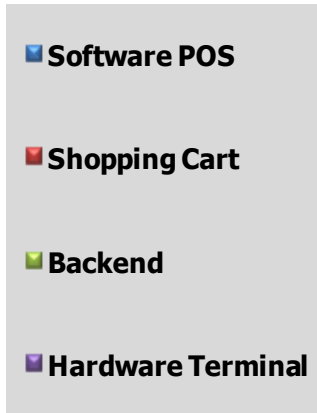
- Food Service
- Retail
- Entertainment
- Travel
- University
- Telecom
- Non-Profit/NGO
- Media
- Petroleum
- Government



**Merchants within the Food Service Industry are the most commonly compromised**  
**Merchants within the Retail Industry are the second most commonly compromised**



# Case Analysis: System Type



None of these systems were  
Visa PABP or PCI PA-DSS compliant

**Software POS** is a system that runs on a PC-based system in a retail environment.

**Shopping Cart** is an e-commerce tool that allows consumers to purchase a merchant's products online.

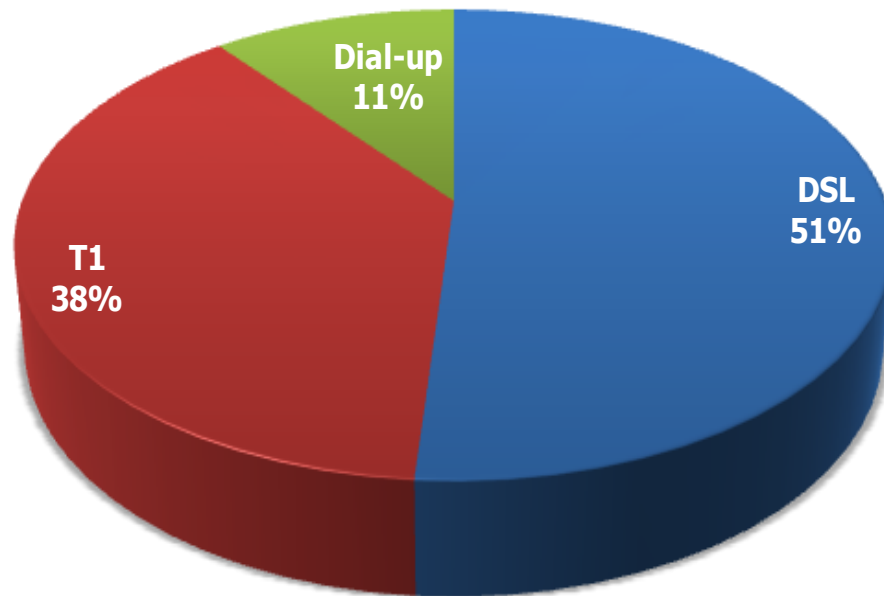
**Backend** is a centralized processing system often called a "transaction switch" used by merchants to aggregate transactions from multiple software POS systems.

**Hardware Terminal** is a dedicated device used by merchants in lieu of a software POS system.



# Case Analysis: External Connectivity

**Trustwave has tracked a high percentage of breaches due to improperly configured remote access via external connectivity.**

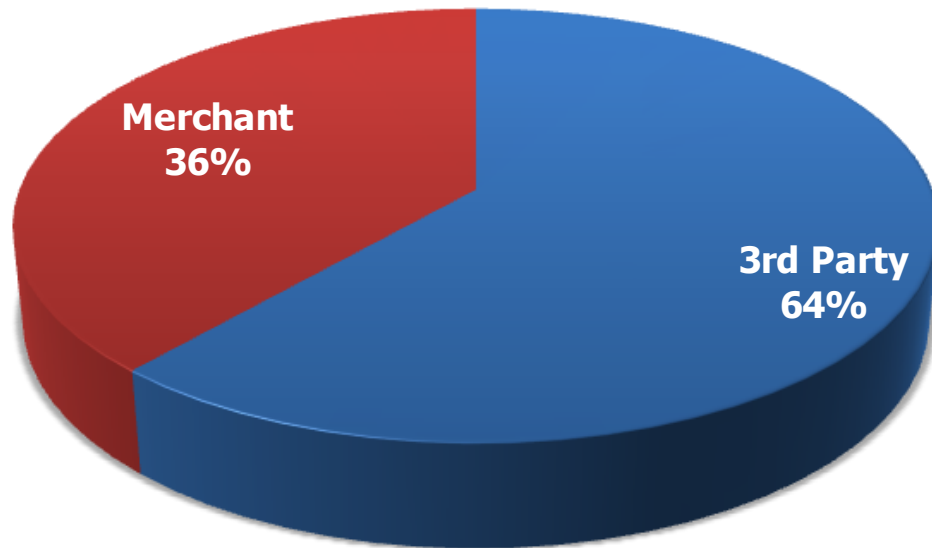


**All Internet connectivity should be considered HIGH RISK**



# Case Analysis: Error

**More than half of the compromises were caused by a fault in the service provided by a 3rd party to the merchant victim.**

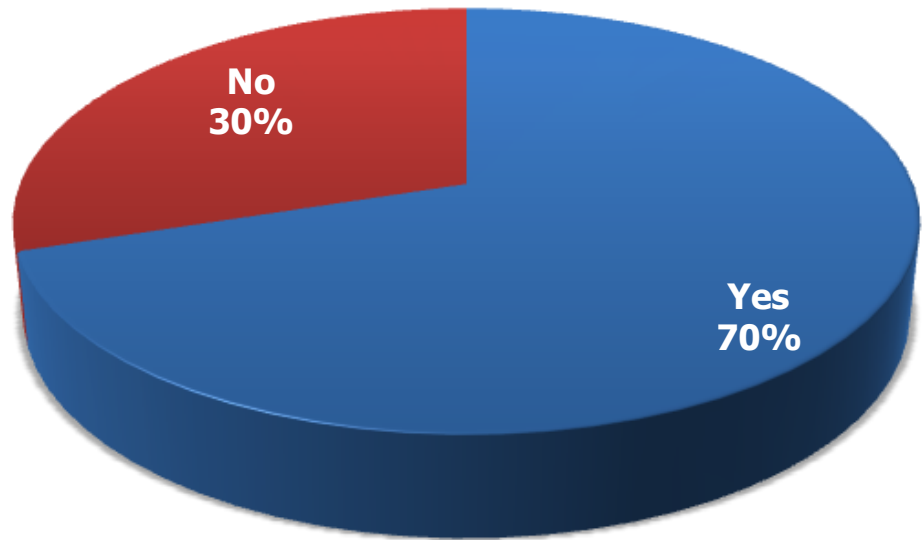


**Some POS developers, integrators, and IT firms  
ARE NOT following PCI DSS and putting Merchants at Risk!**



# Case Analysis: Track Data Storage

**Brick-and-mortar merchants running non-compliant software packages are storing track data and they do not know until it is too late!**

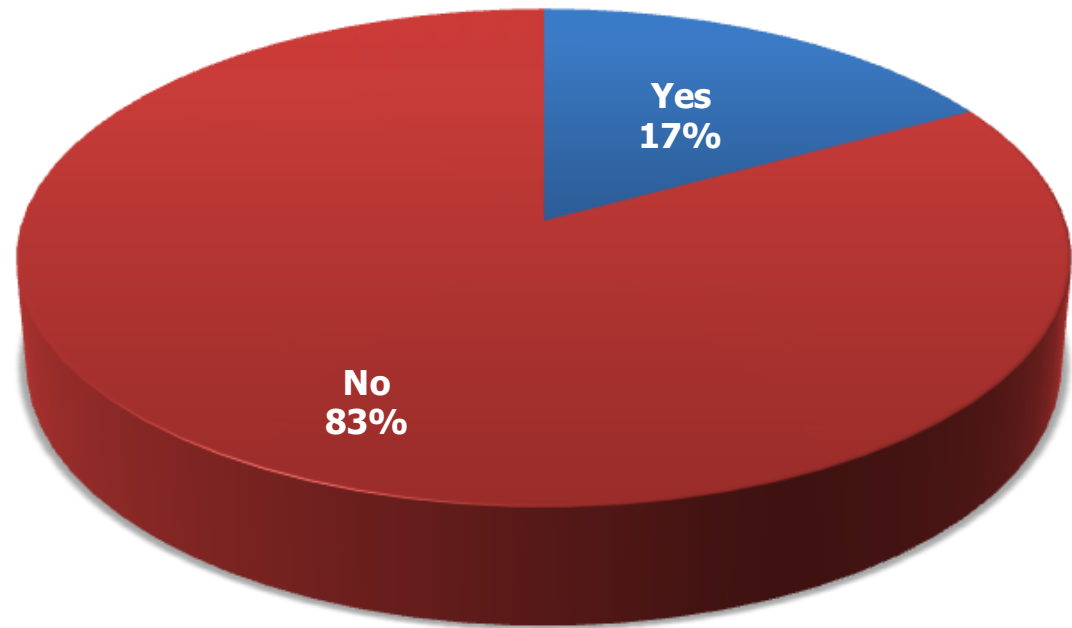


**Track data storage is never permitted in any environment post authorization**



# Case Analysis: Card Validation Code Storage

**Trustwave has found that e-commerce merchants are generally more PCI DSS aware.**



**Card Validation Code storage is never permitted post authorization**



# Top PCI DSS Violations

**Requirement 1:** Install and maintain a firewall to protect cardholder data

**Requirement 3:** Protect stored cardholder data

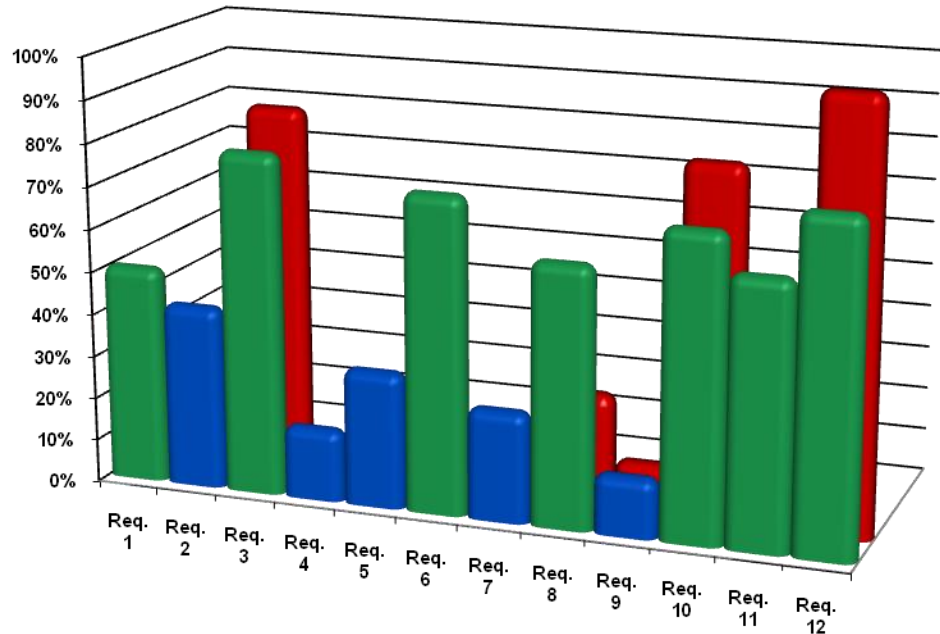
**Requirement 6:** Develop and maintain secure systems and applications

**Requirement 8:** Assign a unique ID to each person with computer access

**Requirement 10:** Track and monitor access to network and card data

**Requirement 11:** Regularly test security systems and processes

**Requirement 12:** Maintain a policy that addresses information security



 Violations >50% Found During Forensic Investigations

 Violations <50% Found During Forensic Investigations

 Violations Found During Initial PCI DSS Audits



# PCI DSS Standard



# Six Goals: Twelve Requirements, PCI DSS

## The “Digital Dozen” the Payment Card Industry Data Security Standard *(1 through 6)*

Build and Maintain a Secure Network	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
Protect Cardholder Data	<ol style="list-style-type: none"><li>3. Protect stored cardholder data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software</li><li>6. Develop and maintain secure systems and applications</li></ol>



# Six Goals: Twelve Requirements, PCI DSS

## The “Digital Dozen” the Payment Card Industry Data Security Standard *(7 through 12)*

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain Information Security Policy	12. Maintain a policy that addresses information security



# The Mandate: Merchant Levels Defined

Level	Merchant Classification Criteria
1	<p><u>Visa &amp; MasterCard:</u> Any merchant-regardless of acceptance channel-that:</p> <ul style="list-style-type: none"><li>• Processes over 6 million Visa or MasterCard transactions per year</li><li>• Has suffered a hack or an attack that resulted in an account data compromise</li><li>• Visa or MasterCard determines who should meet the Level 1 merchant requirements</li><li>• Has been identified by any other payment card brand as Level 1</li></ul>
	<p><u>American Express:</u> Any merchant-regardless of acceptance channel-that processes over 2.5 million American Express transactions</p>
2	<p><u>Visa &amp; MasterCard:</u> Any merchant that processes 1 million to 6 million Visa or MasterCard transactions, regardless of acceptance channel</p>
	<p><u>American Express:</u> Any merchant-regardless of acceptance channel-that processes 50,000 to 2.5 million American Express transactions</p>



# The Mandate: Merchant Levels Defined

Level	Merchant Classification Criteria
3	<u>Visa &amp; MasterCard:</u> Any merchant that processes 20,000 to 1 million Visa or MasterCard e-commerce transactions
	<u>American Express:</u> Any merchant-regardless of acceptance channel-that processes less than 50,000 AMEX transactions
4	<u>Visa &amp; MasterCard:</u> Any merchant that processes fewer than 20,000 Visa or MasterCard e-commerce transactions or processes fewer than 1 million Visa or MasterCard transactions, regardless of acceptance channel



# PCI Self-Assessment Questionnaire



## What is the PCI Self-Assessment Questionnaire?

- A list of questions used to assess your compliance with the requirements of the PCI DSS
- In February of 2008, the PCI Security Standards Council released four versions of the questionnaire to account for different merchant environments
  - SAQ A: Addresses requirements applicable to merchants who have outsourced all cardholder data storage, processing and transmission
  - SAQ B: Created to address requirements pertinent to merchants who process cardholder data via imprint machines or standalone dial-up terminals only
  - SAQ C: Constructed to focus on requirements applicable to merchants whose payment applications systems are connected to the Internet
  - SAQ D: Designed to address requirements relevant to all service providers defined by a payment brand as eligible to complete an SAQ and those merchants who do not fall under the types addressed by SAQ A, B or C



# PCI DSS version 1.2

- Scheduled for availability in October 2008
- Update is based on extensive feedback from the PCI Security Standards Council's participating organizations
- The new version will:
  - Enhance the clarity of its technical requirements
  - Offer improved flexibility
  - Address new and evolving risks and threats



# Next Steps



# Next Steps

## Tips for Small Merchants:

- ✓ **Ask your acquirer/ISO/service provider about PCI DSS compliance**
- ✓ **Ask about resources – many organizations are offering free scanning promotions**
- ✓ **Ask about the POS technology in your store or on your website**
- ✓ **Ask if your payment processor is PCI DSS compliant**
- ✓ **Ask your technology vendor (DSL/Cable provider, hosting provider) about PCI DSS**
- ✓ **Visit the card brand websites to identify compliant entities ([www.visa.com/cisp](http://www.visa.com/cisp))**
- ✓ **Talk to your business association about PCI DSS**

## Tips for Acquirers/ISOs/Service Providers:

- ✓ **Risk Measurement – understand the risk profile across your portfolio**
- ✓ **Embed PCI DSS compliance into your contracts**
- ✓ **Shop around – ask QSAs about tools to manage PCI DSS compliance program**
- ✓ **Communicate to your clients – make sure your merchants are familiar with PCI DSS**
- ✓ **Ask the Card Brands – See what resources they offer for PCI DSS compliance**
- ✓ **Visit the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org))**
- ✓ **Become a participating organization of PCI SSC – provide input**



# **Level Four Merchant Compliance Fifth Third Bank's Perspective**



# Level 4 Merchants – Why They Are So Important

- **Most of Level 1, 2, and 3 merchants are compliant!**
  - Only represent a fraction of the total merchant population
- **The Majority of the Level 4 merchants don't understand:**
  - Today's risks that the payment card industry faces
    - Track data is everywhere
    - This data is very useful to criminals to perpetrate fraud
  - The PCI DSS
  - The value of the PCI DSS validation process



# Payment Applications – Their Importance

- **Many older versions of payment applications still deployed and in use**
- **These older versions often store track data**
  - Remember, this data is of the highest value to criminals
  - Merchants can only store four fields post authorization:
    - Cardholder Name
    - Card Number (must be rendered unreadable)
    - Expiration Date
    - Service Code
- **If a criminal is only able to steal these four pieces of information, the options for committing fraud are fewer**



# Changing Your Risk Profile

- **First, if your company is using a payment application:**
  - Upgrade to a payment application compliant with Visa’s Payment Application Best Practices (PABP)—soon to be the Payment Application Data Security Standard (PA-DSS)
    - Compliant applications do NOT store track data, among other data
  - Ensure your company is not storing historical files containing track data – delete any such files
    - Many breaches have occurred with merchants that upgraded to a compliant payment application but neglected to completely remove and destroy historical files containing track data
- **Second, validate compliance with the PCI DSS**
  - Pay particular attention to:
    - Your perimeter network controls
      - Adequate firewalls need to be in place along with Intrusion Detection/Prevention Systems
    - Any data that you store post authorization
      - Make sure it’s only allowable data
      - Make sure it’s properly protected as per PCI DSS!
      - Better yet, don’t even store it!



# Changing Your Risk Profile

- **Pay particular attention to (cont'd):**
  - How and under what circumstances you transmit credit card data
    - Public networks, which include wireless networks, are of high importance because of the increased potential of data sniffing
    - Public networks, including wireless access points, can be used to get to where you store card data
  - How your web applications are coded
    - Make sure they will accept only certain pre-determined commands
      - Criminals can easily circumvent applications that are designed to accept any database command
  - Your password management policy and processes
    - Weak passwords make it easy for criminals to penetrate even layered security mechanisms!



# Technology Strategies for Reducing Your Risk

- **Tokenization**

- Enables you to store a token rather than the card number
- Removes the value of your stored data to criminals
- How it works
  - You send an authorization to a PCI DSS compliant service provider
  - Your service provider presents the transaction for authorization and returns a unique cross-reference number (I.e., token) back to you in the return message instead of the card number
  - You can use the token to get the full message from your service provider if a specific business reason arises

- **Encrypt the card number at the swipe**

- Encryption needs to be robust (I.e., 3DES 128 bit, AES 256 bit, or DUKPT)
- Key management absolutely critical and must be iron clad!
- At this time, the card brands still consider encrypted card data in scope of the PCI DSS



# Leveraging Your Acquirer, Agent and ISO

- **ALL entities that store, process, or transmit card data must be compliant with the PCI DSS**
  - Make sure your processor, acquirer, agent, ISO, etc. are compliant, as appropriate
  - Understand their ability to support you in your compliance efforts
    - All acquirers are required to have a strategy in place to increase adoption of the PCI DSS and PA-DSS in the Level 4 population
      - Agents and ISO's are important players in this strategy
      - A key point is that all are bound to Visa's new application mandates



# Visa's Payment Application Mandates

- **All merchants are expected to comply with the PA-DSS at all times. In an effort to enforce compliance in regard to payment applications, Visa has issued the following mandates for all Acquirers:**
  - **1/1/08** – Acquirers may not board Merchants who use known vulnerable payment applications.
  - **7/1/08** – Acquirers may certify only PABP-compliant payment applications.
  - **10/1/08** – Acquirers may only board Level 3 and 4 merchants that are PCI DSS compliant and/or use PABP-compliant payment applications.
  - **10/1/09** – Acquirers must decertify all vulnerable payment applications.
  - **7/1/10** – Acquirers may not allow merchants to use non-compliant payment applications on their system.



# Case Study: Fifth Third's Level 4 Merchant Strategy

- **Getting the word out via:**
  - Statement messages
  - Online messages
  - Website messages
  - Merchant welcome kits
  - Partnered with Trustwave to provide multiple webinars
  - Speaking at industry forums
- **Risk assessment methodology in place**
  - Communicating directly with merchants as appropriate
    - Asking for full compliance validation
    - Iterative follow-up to encourage validation
- **Communicating with all merchants using a payment application to upgrade as appropriate**
- **Targeting franchisors to leverage corporate communications to drive adoption across their brand**



**Questions?**